AMENDMENTS TO THE DRAWINGS:

Applicant submits concurrently herewith annotated and replacement drawings illustrating Figs. 1-18.

Attachments: Fourteen (14) sheets of annotated drawings
Fourteen (14) sheets of replacement drawings

REMARKS/ARGUMENTS

Reconsideration of this application is respectfully requested.

In response to continued objection to claims 4 and 12 as being improperly dependent (or independent), these claims have been amended above to be in more traditional dependent format so as to obviate the Examiner's grounds for objection. These claims are clearly proper dependent claims in accordance with all statutory and regulatory requirements.

The allowance of claim 5 is appreciatively noted.

With respect to dependent claims 3 and 11, although the Examiner has continued to include them with others in the broad statement of rejection based on alleged anticipation, the action summary sheet merely objects to these claims, and the detailed comments supporting the alleged anticipation rejections no longer include any discussion of claims 3 and 11. The only particularly stated ground for objection to claims 3 and 11 is their dependence upon a rejected base claim. Accordingly, it is assumed that claims 3 and 11 are also now considered allowable if rewritten in independent form and, thus, no further comment will be made with respect to claims 3, 5 and 11.

The stated rejection of claims 1-4 and 6-15 [sic: 1, 2, 4, 6-10 and 12-15] under 35 U.S.C. §102 as allegedly anticipated by Wedde is respectfully traversed.

The Examiner's detailed comments concerning claims 1, 2, 4, 6-10 and 12-15 are almost exactly quoted from the earlier office action. Insofar as the undersigned can ascertain, exactly

the same citations to Wedde text are made. Accordingly, applicant's earlier given reasons for traversal and already of record are still believed to be appropriate and are hereby incorporated by reference so as not to further burden the record.

In some instances, the Examiner has indicated refusal to give patentable weight to claim recitations reciting apparatus "arranged to" perform a specified function. In some cases, the Examiner's references are obviously inappropriate because the claim does not include such language (see, e.g., the Examiner's comments concerning claim 12 at page 7, lines 4 *et seq.* of the outstanding "final" office action). In the present context, a claim limitation requiring an apparatus to be "adapted to" perform a stated function is believed to be as proper and limiting as requiring an apparatus to be constructed to perform a stated function.

In any event, the above amendment eliminates all such language in favor of more positive recitations. Accordingly, the Examiner is respectfully requested to give patentable weight to such recitations.

The Examiner replied to applicant's arguments at page 14 of the submission filed on December 21, 2007, as being insufficiently specific – thus constituting a failure by applicant to carry the burden of proving that the Examiner has failed to make out a *prima facie* case of anticipation. Accordingly, an even more specific traversal will now be provided.

The Examiner's response to applicant's arguments at pages 14-15 of the prior submission ignores step (b) of claim 1 by starting the discussion only at element (c). However, claim 1 (b) requires "receiving semantic data representing a graph structure of hierarchical semantic

relationships between available system commands, including those in the set of system operating rules." The only portions of Wedde asserted by the Examiner to anticipate this recitation in claim 1 are 97, Abstract at lines 6-19; 97:2:18-43; 99-100, §§3.1 and 3.2; and 102 at §4.5. All of this cited language is quoted below for convenience.

> "...In this paper we introduce a distributed authorization concept which is based on a modular authorization language for supporting cooperating *distributed authorization teams*. These teams are partially ordered into a hierarchy in that they inherit authorization rules from higher order teams but still exercise their autonomy by (dynamically) setting local rules that serve the special local needs in distributed organizations. *Conflicts* between [between: sic] rules inherited from different higher ranking sources, or *violations* of higher order rules through local rules would be detected, on the logical level or through request evaluation, as contradictions or contradicting results, respectively. Conflict resolution mechanisms are presented, and examples are discussed extensively.
>
> * * *
>
> ...The implementation of these concepts are part of our DRAGON SLAYER project, a distributed file system which supports the needs of large heterogeneous [heterogenous: sic] and decentralized organizations [10]. Here, a **modular** authorization *enables the administrative teams to specify the access control in a distributed environment like the* DRAGON SLAYER *system, through sets of rules.* Authorization teams may be located in, or associated with, any department or work group of an organization.
>
> * * *
>
> In order to represent their influence we define **authorization spheres**. We incrementally and adaptively model, in the DRAGON SLAYER file system, a very general framework of distributed authorization policies, through relations of roles, groups, and authorization spheres. While role patterns may help to model authorization mechanisms in an organizational group these patterns may also be autonomously refined, modified, or adapted by the local administrators in order to fulfill the special needs of the group.
>
> * * *

3.1 Groups and Roles

As in other models that are based on role-based access control (RBAC) [8] 'a *role* is a job function or job title within the organization with some associated semantics regarding the authority and responsibility conferred on a member of the role'. In our approach we additionally – and in contrast to [7][1] – define *groups* to model organizational units such as departments or project groups.

We recognize that a user may play different roles in different groups, e.g., a 'developer' of the group 'network' may temporarily also be a 'programmer' of the group 'crypto'. If the access rights would only refer to a role, this user would be granted access to objects of the group 'crypto' which are restricted to the role 'developer' of this group. This may be undesirable. Thus the access rights, or limitations, for a particular person will be specified w.r.t. his or her membership in a group, project team etc. Consequently, every access right will be specified to apply to a pair *((role), (group))*. For the purpose of formal specification we consider a group as a set of subjects and objects to pursue (possibly very complex) tasks. While objects are the data files needed for the task subjects are individuals who may manipulate the objects according to their roles in the group.

The roles in our scenario are ordered hierarchically as shown in figure 3. Access rights will be formulated according to this hierarchy in such a way that typically access privileges are higher ranking roles would not be available in lower capacities while through their higher ranking, individuals *may* automatically have access rights associated with lower ranking roles. Also the holders of different roles in separate groups may have to be prevented from exercising privileges of a higher role in one group (e.g., 'developer') while acting in a lower role (e.g., 'programmer' in another group (as mentioned in the beginning of 3.1). *Every time access to an object o is requested all authorization rules referring to o are checked.*

3.2 Authorization Spheres

One new aspect of our modular authorization language is a decentralized definition of the access policies through local authorization teams. The

[1] In [7] groups are set of users and a group can be assigned to roles. Thus the role is [a: sic] assigned to all users which are members [member: sic] of the group.

access policy of a local authorization team, expressed through a set of rules, should be valid for a well-defined set of subordinate groups or their organizational functions. We call this the **authorization sphere** of an authorization team. An authorization team consists of all users who jointly may modify the set of rules of this authorization sphere. *An authorization sphere is a special group,* e.g., 'marketing' in figure 2. However, while every group is within an authorization sphere we may consider, in figure 2, the group 'web' not to have an independent authorization team. Authorization spheres do not overlap.

In our model the authorization is partially done in a **modular** fashion, through the different authorization teams. At the same time we have an **inheritance principle** built into our model, which is based on hierarchical relationships between authorization spheres. In detail:

3.2.1 If a group has an authorization team which could define rules for accessing and manipulating objects then these rules are valid for the group, as well as for subordinate groups.

3.2.2 The autonomy of each authorization team is constrained by the rules defined by any authorization team in a supervisory group. In particular violations of superseding rules should be detected, and finally be removed (since inherited rules will hold anyway but in case of conflicts). We assume that the problem of violations in the context of our discussion (i.e., *not* for shaping the rule design process!) would occur during rule evaluation while handling authorization requests. This is beyond the scope of this paper.

3.2.3 In a group hierarchy the group of the highest order has an authorization team.

3.2.4 If two inheritance streams are merged into a subordinate authorization sphere this may lead to **conflicts** in the corresponding components, in that access to a particular object may be granted according to one inherited rule set while defined according to the other. As an obvious assumption we have to assume that the inherited rules from the one and the other stream both apply to common subjects and objects, that were [where: sic] already

> addressed in supervisory authorization spheres. A conflict resolution is required that determines which of the conflicting rules applies.
>
> In order to model these conflict resolutions every group which inherits from two or [ore: sic] more superordinate authorization spheres must have an authorization team of its own.

4.5. Evaluation of access requests

The key features for granting or denying an access request are the grant rules. In detail:

Assuming a request of subject *s*, for processing object *o* by using method *a*, arrives at the sites that hold copies of the object. The corresponding authorization sphere [would] be *as*.

1. It will be checked for which grant rule in *as*, *a* is a matching method. If there is none the integrity of the rules is violated, and the response is 'error'.
2. For the resulting grant rules under further inspection, their right sides will be checked whether the particular triple (*s, o, a*) of the request is legal for each predicate L_i in a configuration constituting a grant rule. (This involves an iterative process in evaluating rules according to definitions 13 – 16.)
3. The resulting L_i will be evaluated.
4. If an expression of the form $L_1\&..\&L_n$ has been identified where the L_i are valid rules then the corresponding grant rule is valid.
5. If one grant rule with expression $L_1\&..\&L_n$ is evaluated to be valid and positive then the result 'accept' is transmitted to *s*. If the evaluation result is negative then 'deny' is transmitted.
6. If different grant rules have conflicting results (a so far undetected conflict of violation) the response is 'error'.

Please note that the iteration mentioned in 2) halts. The scope of the access rules in definitions [definition: sic] 13 – 17 is growing yet the evaluation of a *cando* rule halts (only feature predicates), *dercando* contains only feature predicates or *cando* etc.

As will be observed, there is nothing in any of the above-quoted text which teaches a method of identifying conflicts in a set of system operating rules which includes, *inter alia*, step (b) of claim 1 – requiring receipt of semantic data representing a graph structure of hierarchical semantic relationships between available system commands, including those in the set of system operating rules.

Indeed, the only hierarchy described in Wedde is found in other sections of the paper where the hierarchy of the authorization spheres is depicted (figure 1) and/or the "group hierarchy" is depicted (figure 2) or the "role hierarchy" is depicted (figure 3). None of these hierarchical relationships represent a graph structure of relationships between available system commands, including those in the set of system operating rules. Instead, these all appear to be related to the hierarchical relationships between people/organizations within a software development company.

Indeed, the only "conflict resolution" teaching in this paper is found at sections 5 and 6.2. Here, one class of conflicts (rules created in a lower authorization sphere contradicting one inherited from a higher authorization sphere) is said to be removed or voided by "conventional approaches." The other class of conflicts (rules inherited from more than one authorization sphere contradicting) appears to also rely upon collaboration between humans to "resolve the problem" – "in appropriate ways."

If the Examiner believes that Wedde teaches methodology which requires, *inter alia*, receiving semantic data representing a graph structure of hierarchical semantic relationships

between available system commands, including those in the set of system operating rules, then it is respectfully requested that the Examiner identify more particularly and distinctly exactly where such teaching resides in the Wedde reference. What are the system commands – and what is the semantic data representing a graph structure, etc.?

Perhaps the Examiner was attempting to find such by offering the following comment:

> "The access hierarchy is a graph structure. Inheritance of authorization rules (semantic data) will provide a semantic relationship in the hierarchy..." [Page 5, lines 14 *et seq.*]

However, the undersigned has been unable to find reference to any "access hierarchy" in the Wedde paper. If the Examiner is referring to a hierarchical relationship between those humans or groups of humans who are permitted to have access rights (e.g., based upon the task of each role in a project team), it is respectfully noted that such a hierarchy of human resources is not semantic data representing a graph structure of hierarchical semantic relationships between available system commands, including those in the set of system operating rules.

With respect to element (c) of claim 1, the Examiner alleges that Wedde's reference to rule inheritance inherently expands rules "according to allowable semantic relationships (the inheritance relationship)." However, while the inheritance of rules may well lead to an increased number of rules, that clearly does not expand the set of system operating rules being analyzed according to allowable hierarchical relationships between available system command portions, to

give, for any particular system operating rule, an additional system operating rule for each hierarchical semantic level in the graph structure below the system command present in the particular rule – as required by claim 1. Indeed, the Examiner's discussion appears to confuse hierarchical relationships between humans (e.g., "teams" or "sources") and hierarchical semantic relationships between system commands.

In any event, claim 1 (c) explicitly requires the creation of an additional system operating rule for each hierarchical semantic level in the graph structure below the system command present in the particular rule being analyzed and expanded. Clearly, mere "inheritance" of additional rules from some other team of humans does not in any way teach or suggest this aspect of applicant's claim 1.

The Examiner questions applicant's earlier explanation that Wedde fails to teach the specifically claimed features of applicant's invention by arguing that the claim language is so broad and general that there is no claimed "specific" way of solving conflicts recited in applicant's claims.

With all due respect, the Examiner is requested to review applicant's claim 1 requirements. Claim 1 (b) specifically requires receipt of semantic data representing the graph structure of hierarchical semantic relationships between available system commands, including those in the set of system operating rules being examined. Claim 1 (c) requires expanding those system operating rules so as to give, for any particular system operating rule, an additional system operating rule for each hierarchical semantic level in the graph structure below the system

command present in that particular rule. Claim 1 (d) also requires comparison between the specified expanded system rules (i.e., conforming to the claim 1 requirements) to identify those rules for which a semantic conflict occurs therebetween.

As to the final step of claim 1, the Examiner refers to Wedde at 97:Abstract, 6-19; 97:2:18-98:5; 99 at §3.2 and 102-103 at §5.

First of all, the Wedde "inherited" rules do not qualify as the claimed "expanded" rule set. As previously explained, claim 1 requires the expansion process step to give, for any particular system operating rule, an additional system operating rule for each hierarchical semantic level in the graph structure below the system command present in that particular rule. Merely inheriting additional rules from some other source does not provide the claimed expanded rule set. Therefore, it is impossible for Wedde to teach comparison of the "expanded system rules" so as to identify rules for which a semantic conflict occurs.

Secondly, the "conflict resolution" section 5 cited by the Examiner at pages 102-103 makes clear that the Wedde "principle for conflict handling is that all involved authorization teams in the affected spheres have to collaborate to resolve the problem." [Page 102, col. 2, section 5, third full paragraph.]

The Examiner is also referred to dependent claim 2 which adds even more specificity to the claimed methodology of claim 1. In particular, claim 2 requires, *inter alia*, when any of the system rules identify more than one system user in the subject portion, and/or more than one system object in the object portion, then such rules must be expanded to produce replacement

rules having a single system user in the subject portion, and a single system object in the object portion, said replacement rules being produced before the parent claim 1expansion step (c) is performed.

Claim 4 specifically requires the claimed method to further comprise generating a set of system operating rules by resolving any identified conflicts in the expanded set of initial rules to give a resolved expanded set of operating rules. As already noted above, claim 1 specifically requires the expanded set of operating rules to include an additional system operating rule for each hierarchical semantic level in the graph structure below the system command present in that particular rule.

Apparatus claims 9, 10 and 12 have obvious analogy to method claims 1, 2 and 4, respectively. In addition, the apparatus claims are drafted in "means-plus-function" form as permitted under 35 U.S.C. §112, 6th paragraph. Accordingly, these claims are directed to the specific corresponding structure described in the specification and equivalents thereof. As such, these claims are even more patentably distinct from any possible teaching or suggestion of Wedde.

With respect to the Examiner's more general arguments about proper examination procedure, it is respectfully submitted that the Examiner has failed to interpret the rejected claims with their broadest reasonable scope in light of the supporting disclosure. This observation is especially pertinent with respect to the apparatus claims drafted in "means-plus-function" form. However, even with respect to the method claims, while applicant is not asking for limitations appearing in the specification to be read into the claims, the applicant is respectfully requesting

that a "reasonable" interpretation be given to all explicit claim recitations. For reasons noted above, it is believed that the Examiner's stated grounds of rejection with respect to Wedde are based upon either misinterpretation of Wedde or an over-broad, unreasonable claim construction for the rejected claims.

Accordingly, this entire application is now believed to be in allowable condition, and a formal notice to that effect is respectfully solicited.

Respectfully submitted,

NIXON & VANDERHYE P.C.

By: Larry S. Nixon

Larry S. Nixon
Reg. No. 25,640

LSN:lef

901 North Glebe Road, 11th Floor
Arlington, VA 22203-1808
Telephone: (703) 816-4000
Facsimile: (703) 816-4100

ANNOTATED MARKED UP DRAWINGS FOR SN 10/531,054

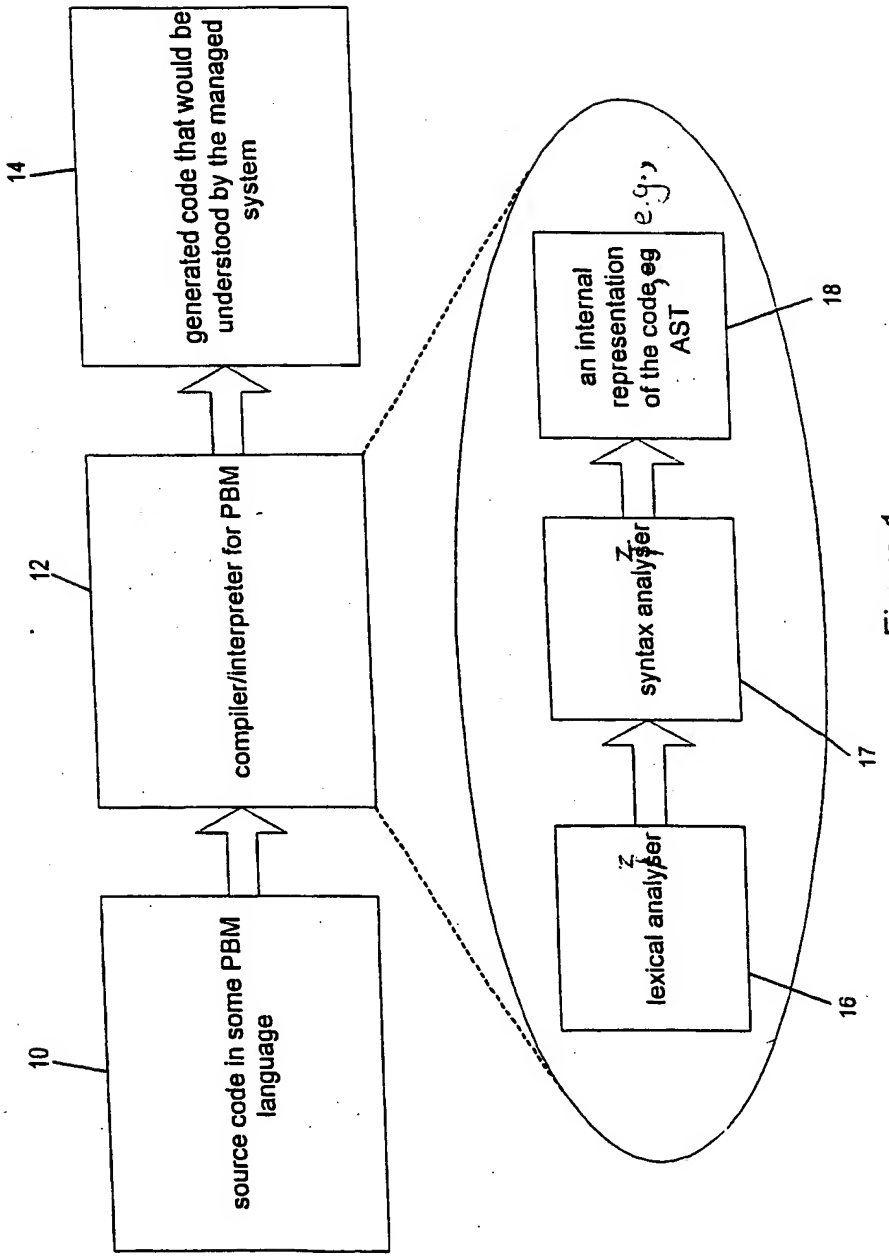


Figure 1 (PRIOR ART)

ANNOTATED MARKED UP DRAWINGS
FOR SN 10/531,054

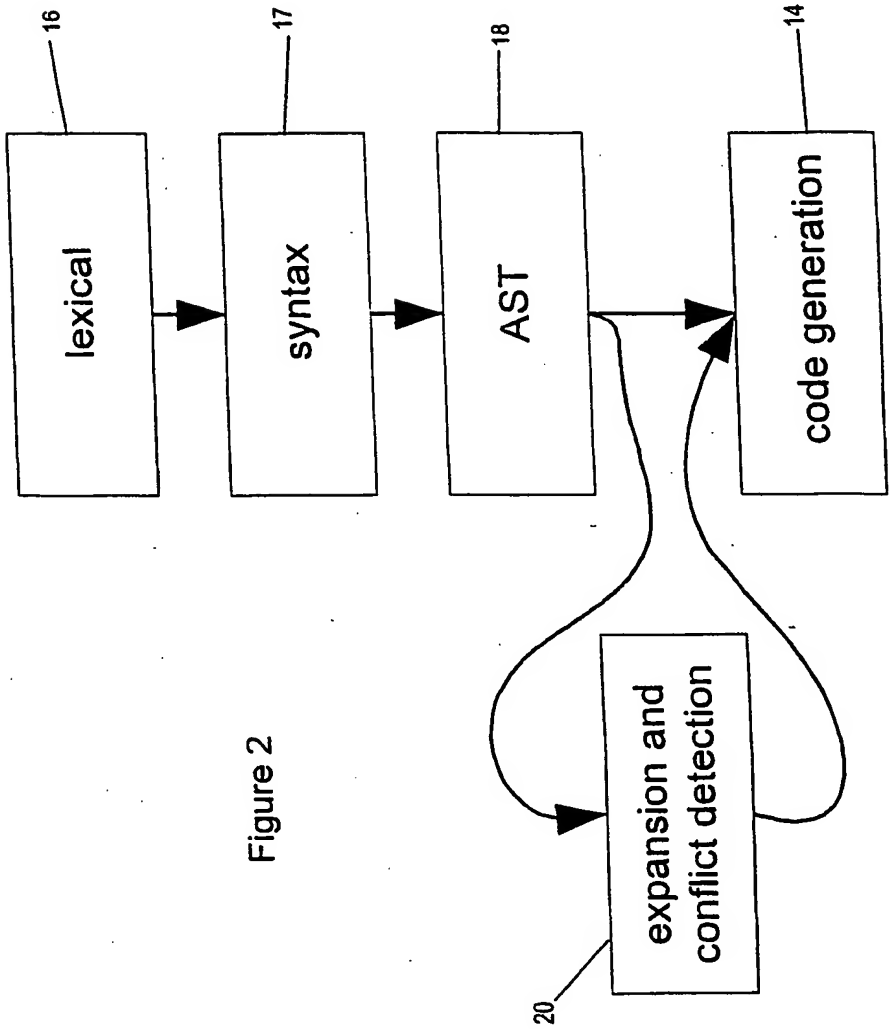


Figure 2

ANNOTATED MARKED UP DRAWINGS
FOR SN 10/531,054

Remove shading

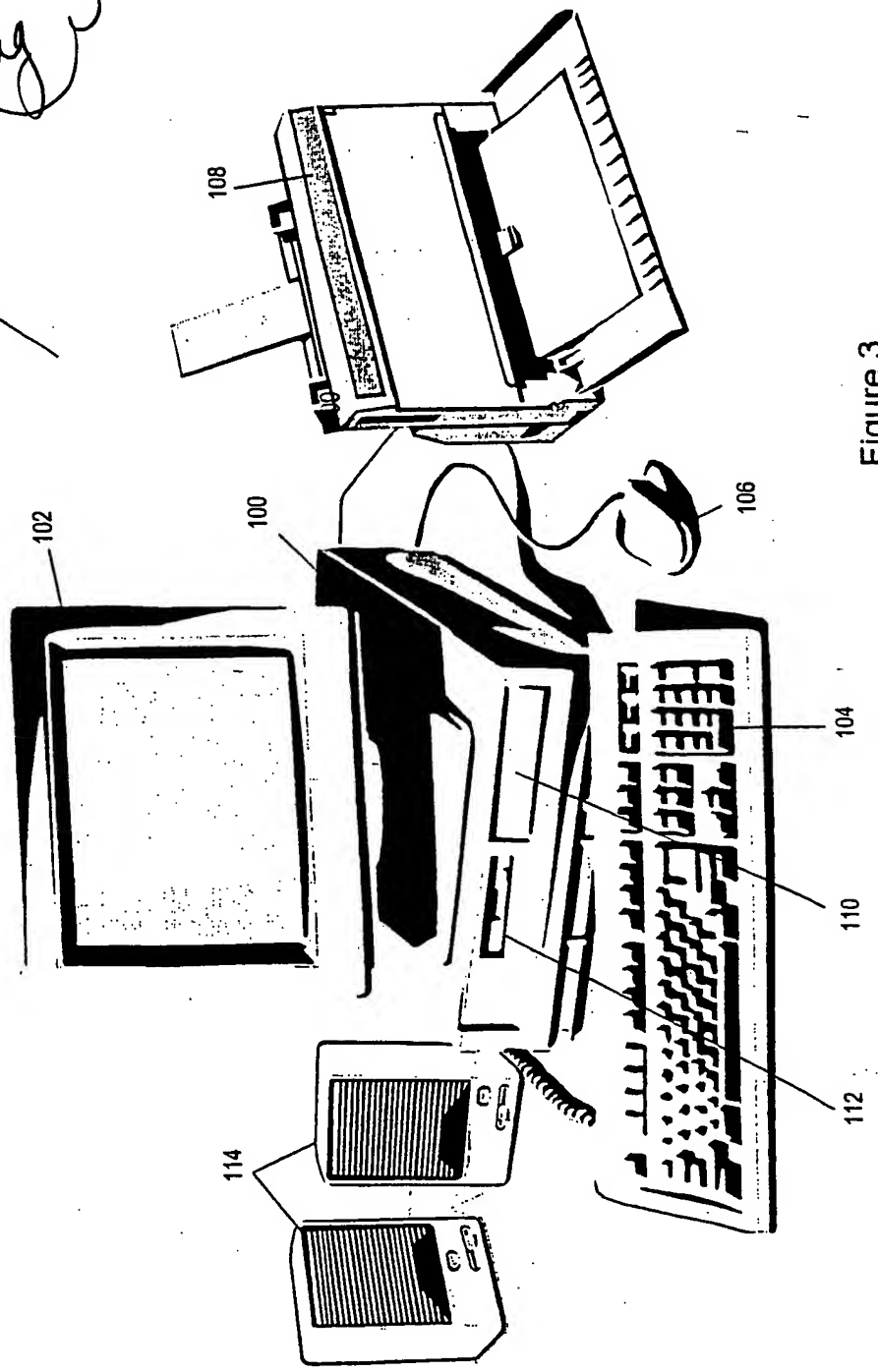


Figure 3

ANNOTATED MARKED UP DRAWINGS
FOR SN 10/531,054

Remove shading

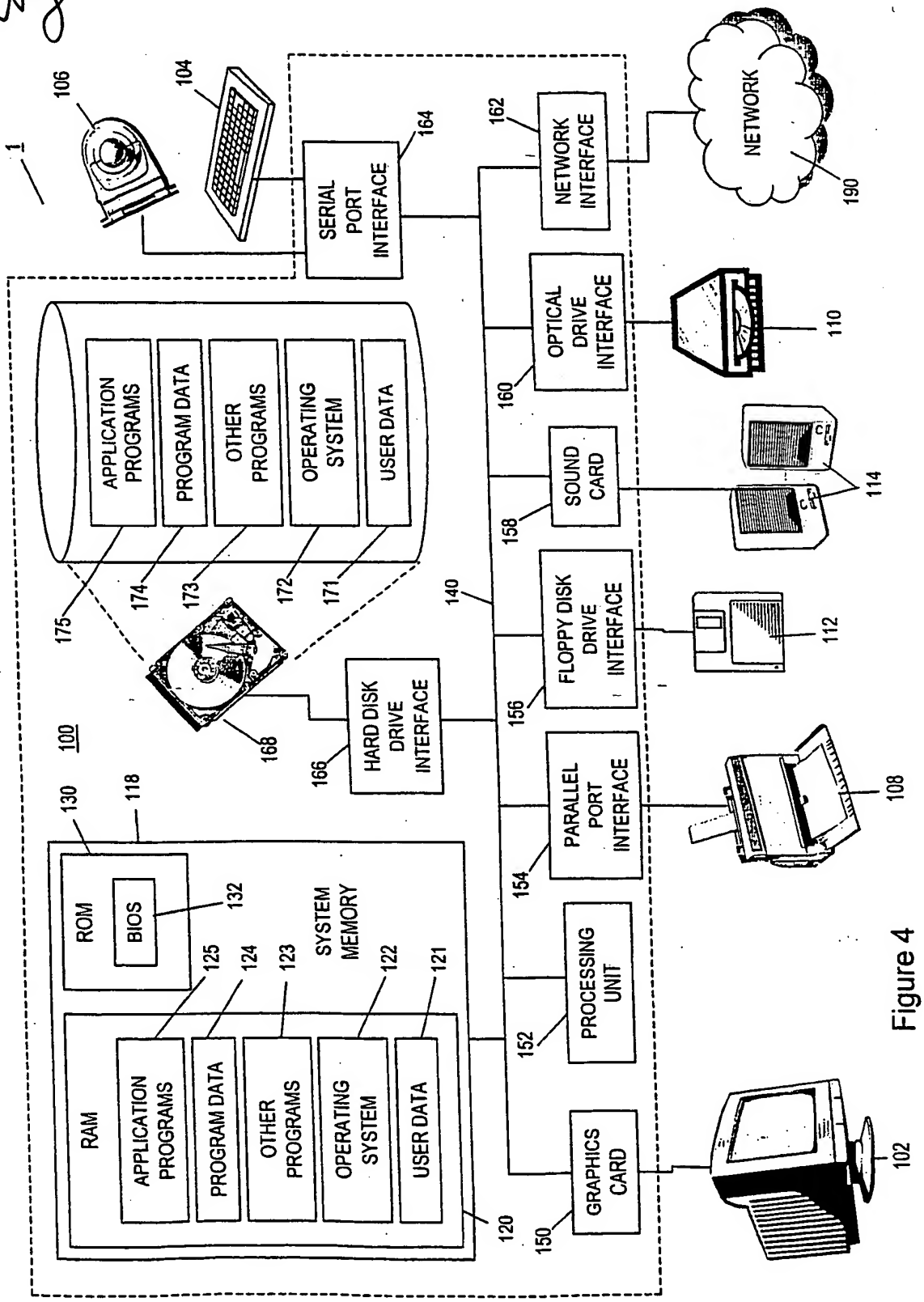


Figure 4

ANNOTATED MARKED UP DRAWINGS
FOR SN 10/531,054

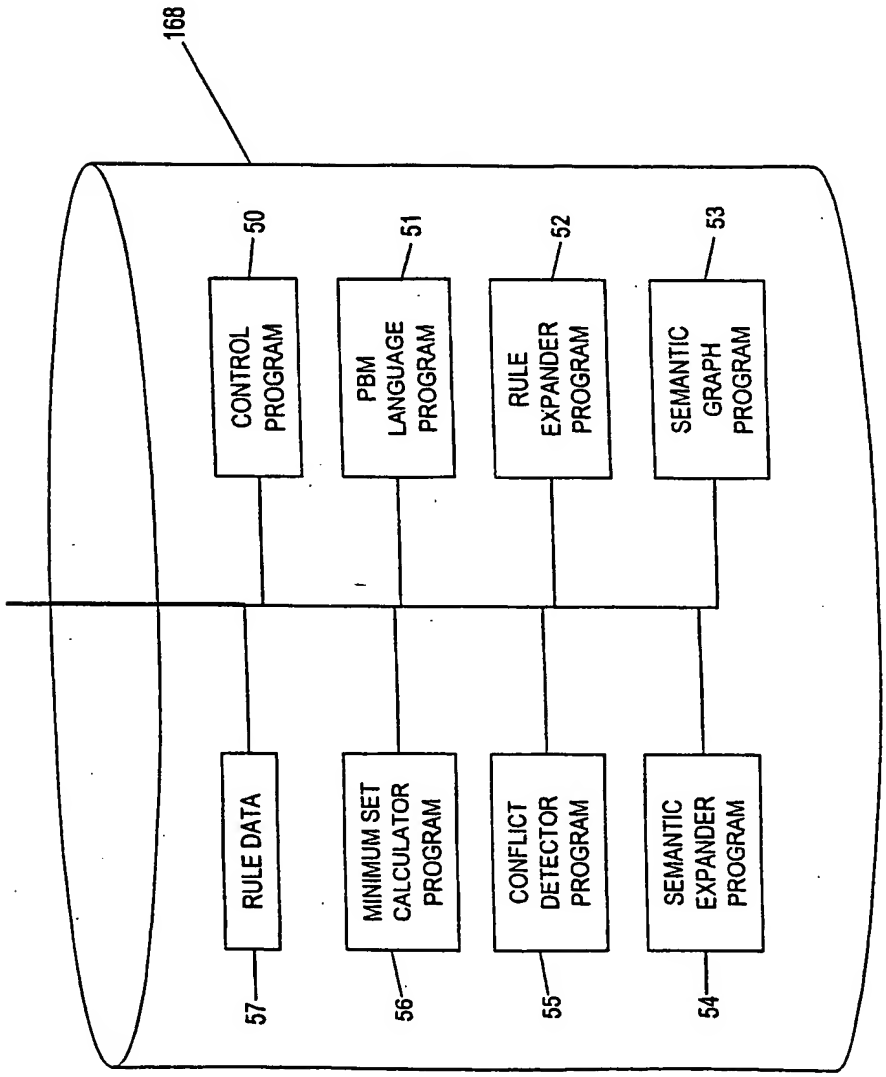


Figure 5

ANNOTATED MARKED UP DRAWING
FOR SN 10/531,054

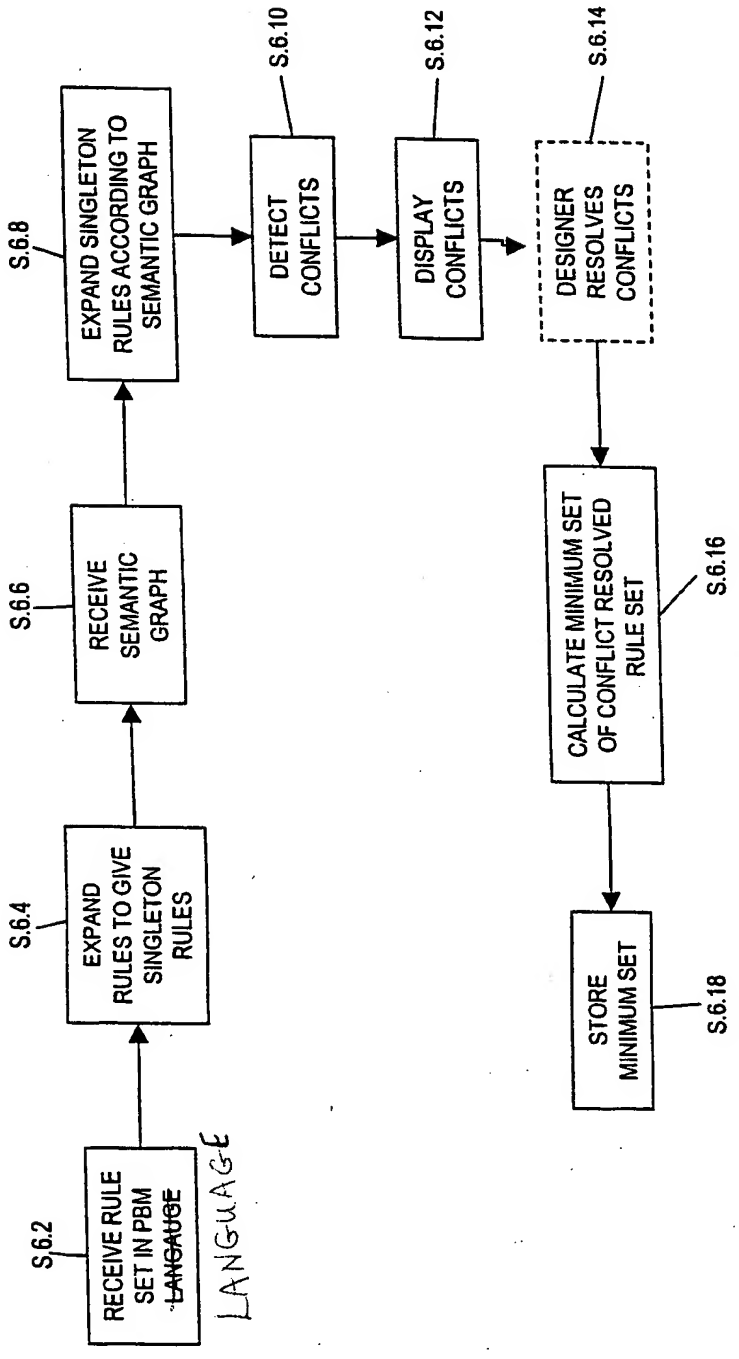


Figure 6

ANNOTATED MARKED UP DRAWINGS
FOR SN 10/531,054

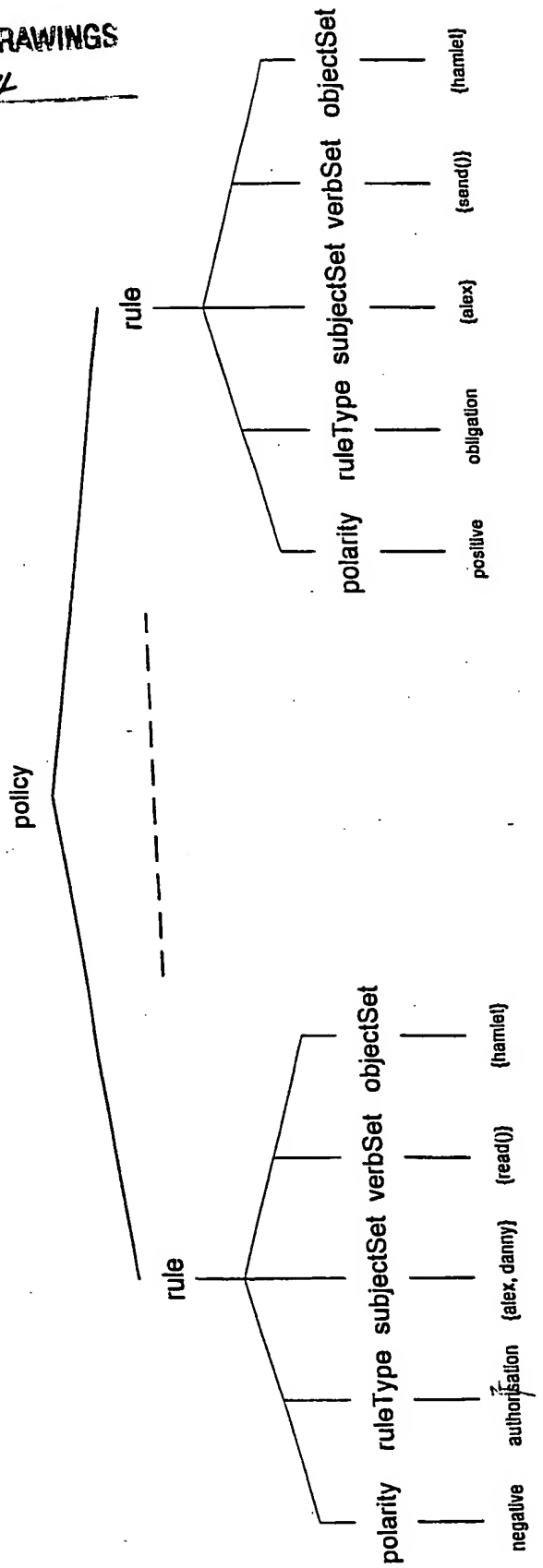


Figure 7

ANNOTATED MARKED UP DRAWINGS
FOR S/N 10/531,054

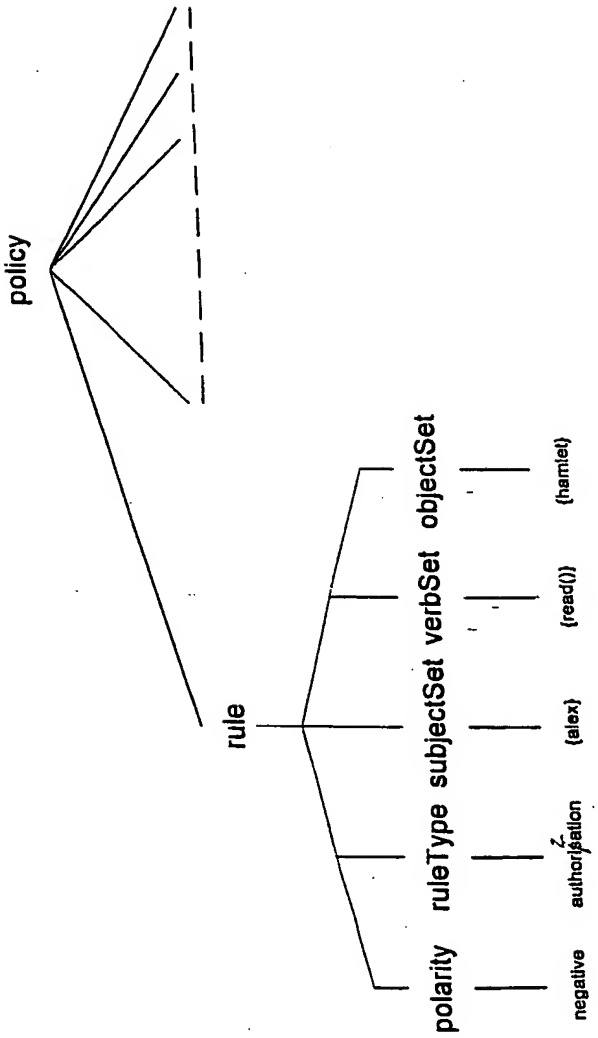


Figure 8

ANNOTATED MARKED UP DRAWINGS
FOR SN 10/531,054

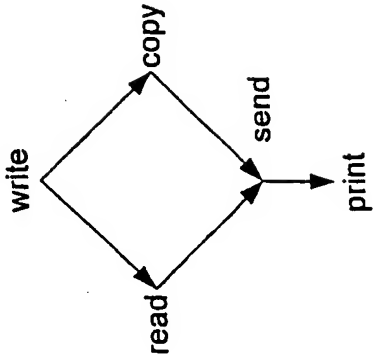


Figure 10

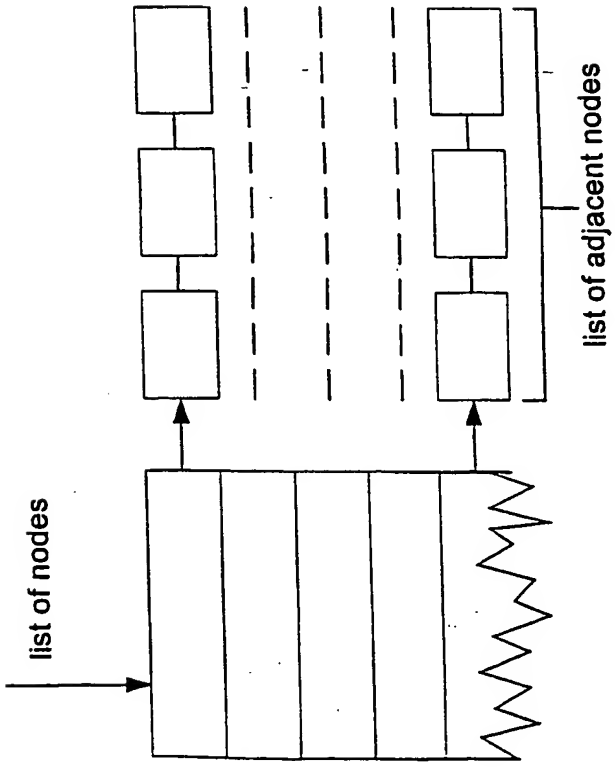


Figure 9

ANNOTATED MARKED UP DRAWINGS
FOR S/N 10/531,054

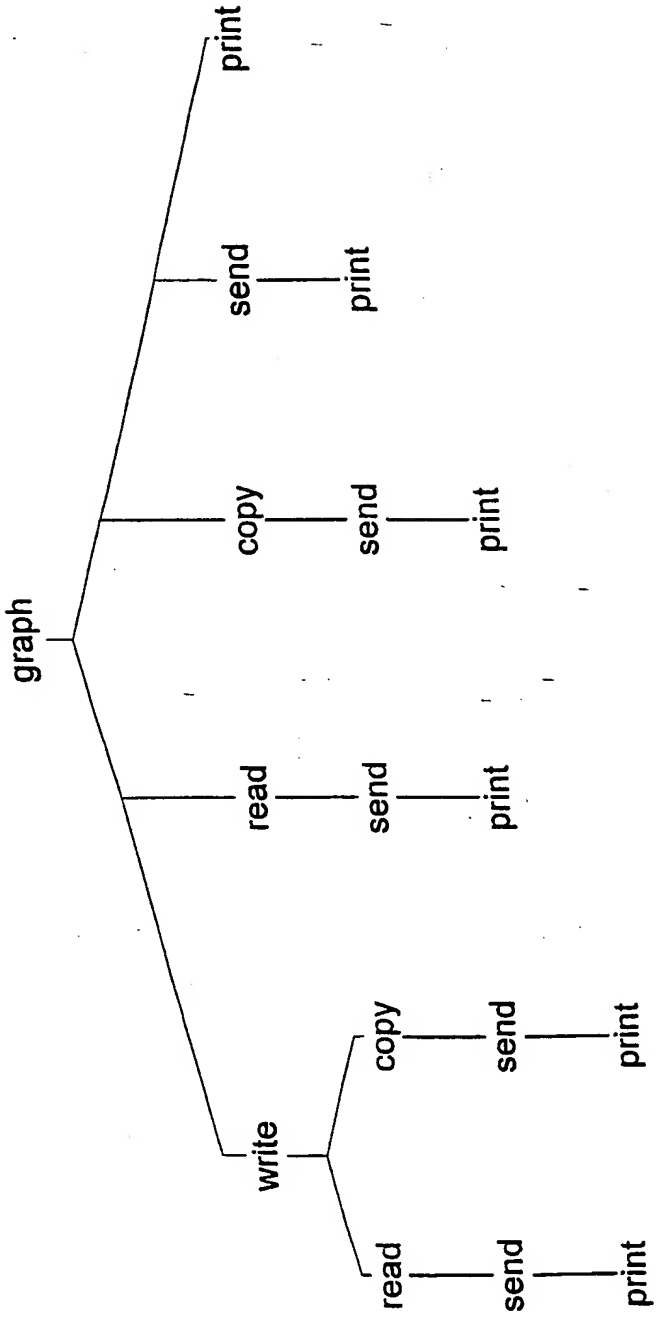


Figure 11

ANNOTATED MARKED UP DRAWINGS
FOR SN 10/531,054

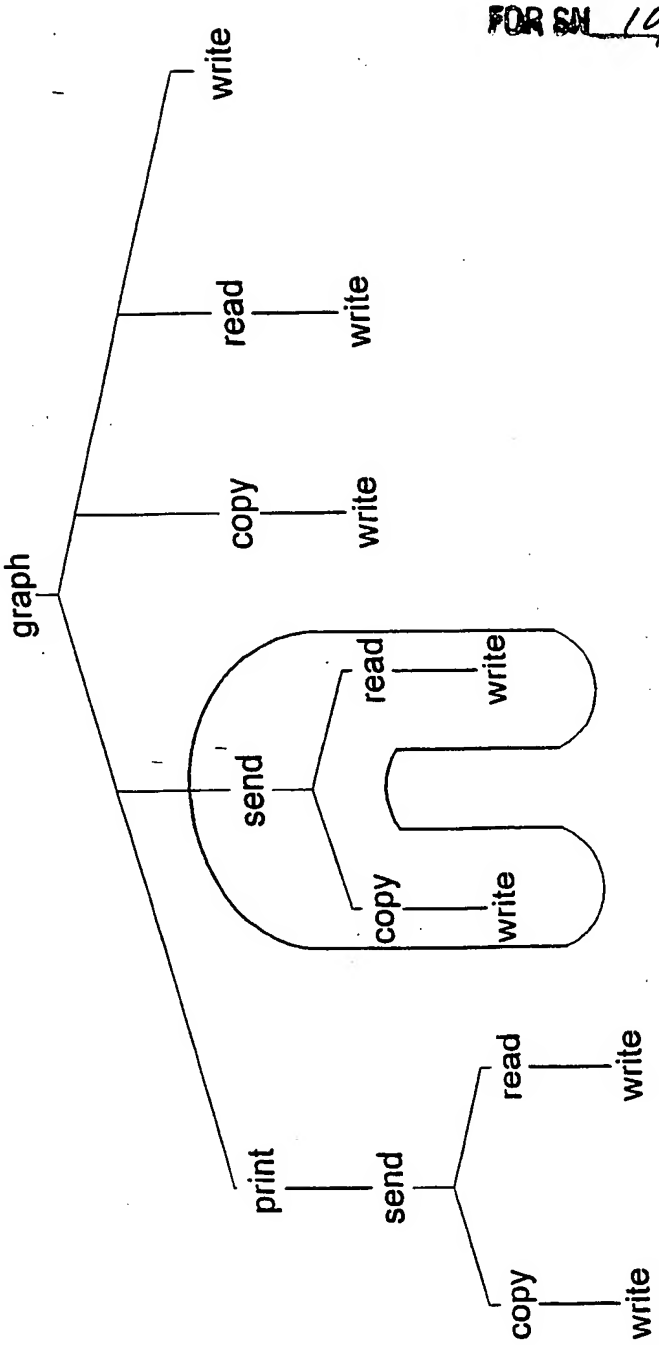


Figure 12

ANNOTATED MARKED UP DRAWINGS
FOR SN 10/531,054

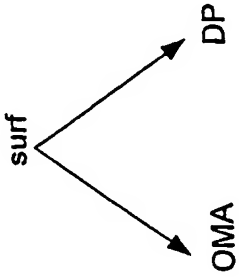
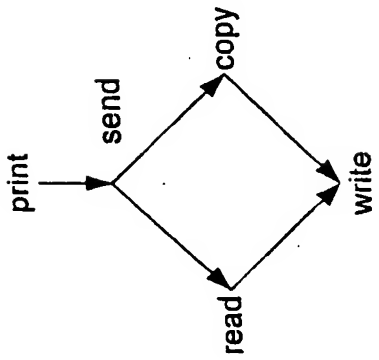


Figure 14



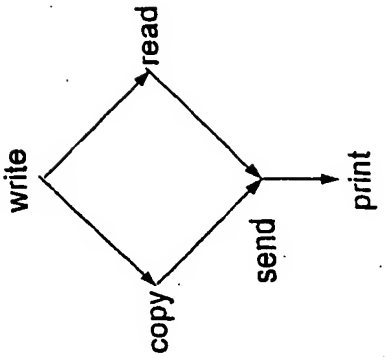


Figure 15

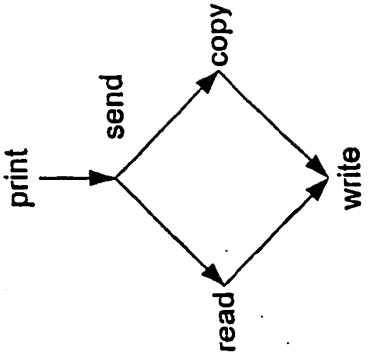


Figure 13

ANNOTATED MARKED UP DRAWINGS
FOR SN 10/531,054

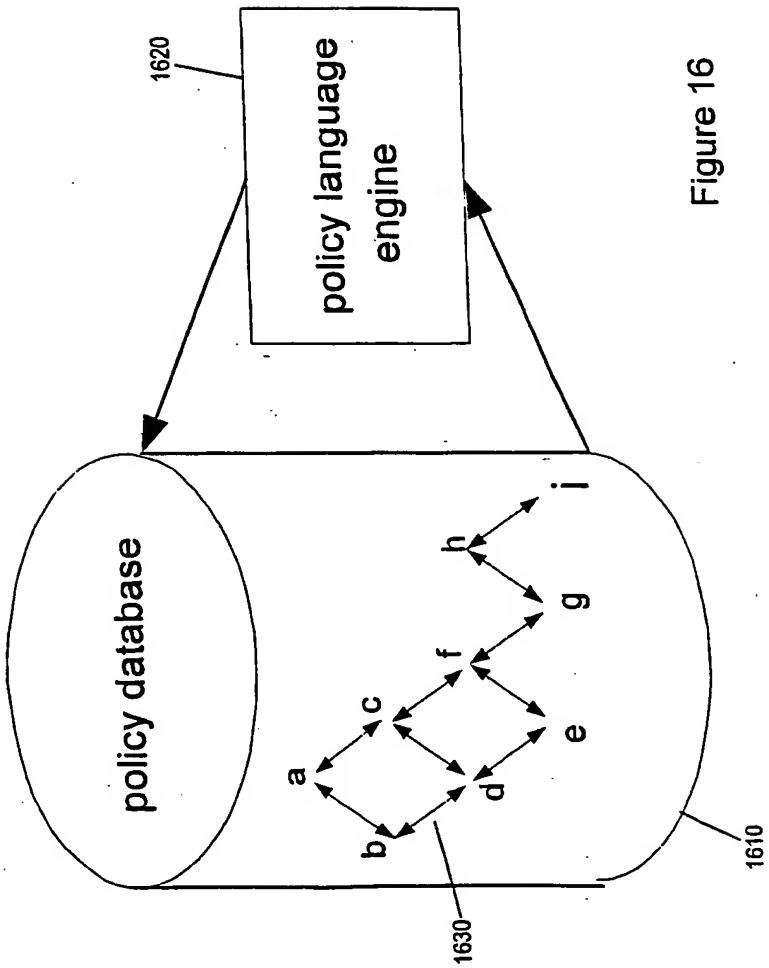


Figure 16

ANNOTATED MARKED UP DRAWINGS
FOR S/N 10/531,054

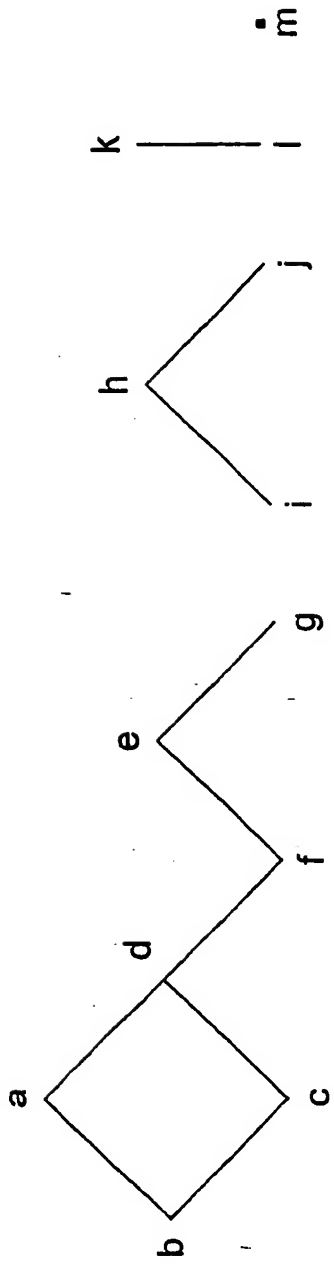


Figure 17

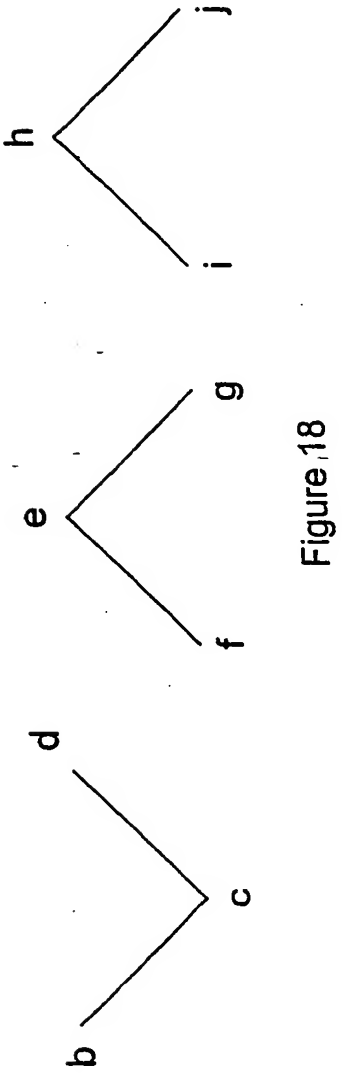


Figure 18